REMARKS

Upon entry of this Response, claims 1-23 remain pending in the present patent application. Applicants respectfully request reconsideration of the pending claims in view of the following remarks. In item 3 of the Office Action, claims 1, 3-8, 10-15, 17-20, 22, and 23 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication 2002/0122553 A1 filed by Kao et al. (hereafter, "*Kao*"). Anticipation under §102 "requires the disclosure in a single prior art reference of each element of the claim under construction." W.L. Gore & Associates, Inc. v. Garlock, Inc., 220 USPQ 303, 313 (Fed. Cir. 1983). For the reasons that follow, Applicants respectfully assert that *Kao* fails to show or suggest each of the elements of the above-mentioned claims. Accordingly, Applicants request that the rejection of these claims be withdrawn.

To begin, claim 1 as originally filed states as follows:

> 1. A method for providing access to an application, comprising the steps of:
>
> encrypting at least one authentication sequence in a computer system using a first network identifier as an encryption key;
>
> storing the encrypted at least one authentication sequence in a memory accessible to the computer system;
>
> decrypting the encrypted at least one authentication sequence using a second network identifier as a decryption key, the second network identifier being procured after storing the encrypted at least one authentication sequence; and
>
> performing an expedited login task to access the application with the at least one authentication sequence if the decryption of the at least one authentication sequence is successful.

With respect to claims 1, 8, 15, and 20, the Office Action states:

> 4. As per claims 1, 8, 15 and 20, Kao teaches a method/system for providing access to an application, comprising the steps of:
>
> encrypting at least one authentication sequence in a computer system using a first network identifier as an encryption key (i.e., encrypting a password using user's minor key) [paragraphs 0047 and 0049];
>
> storing the encrypted at least one authentication sequence in a memory accessible to the computer system (i.e., storing the encrypted password) [paragraphs 0047 and 0049];
>
> decrypting the encrypted at least one authentication sequence using a second network identifier as a decryption key, the second network identifier being procured after storing the encrypted at least one

> authentication sequence (i.e., decrypted the encrypted password using a regenerated minor key) [paragraphs 0050-0051]; and
>
> performing an expedited login task to access the application with the at least one authentication sequence if the decryption of the at least one authentication sequence is successful (i.e., providing the password to access a resource) [paragraph 0051].
>
> 5. As per claims 3, 4, 10, 11, 17, 18, 22 and 23 Kao further teaches the method/system wherein the step of performing the expedited login task to access the application with the at least one authentication sequence further comprises the steps of: executing an automated login to access the application using the at least one authentication sequence and executing the application if the automated login is successful [paragraph 0051].
>
> 6. As per claims 5-7, 12-14 and 19, Kao further teaches the method/system further comprising the step of procuring the first network identifier, the first network identifier being a network address that varies based upon a network coupling status of the computer system [paragraph 0050].

Office Action of November 28, 2006, pp. 2-3. Applicants respectfully disagree. In particular, as set forth in claim 1, the authentication sequence is encrypted using a first network identifier as an encryption key. Thereafter, in decrypting the encrypted authentication sequence, a second network identifier is employed as the decryption key. In this respect, the encryption key and the decryption key could differ, since the first and second network identifiers might change if the computer system has been relocated. Such might be the case, for example, if a person steals a computer coupled to a first network and attempts to attach it a second network or it is not coupled to a network at all.

Thus, the network identifiers that are used to encrypt or decrypt an authentication sequence are identifiers that are associated with the networks to which the computer system is coupled. Assuming that the computer system is coupled to the same network when both the first and second network identifiers are obtained, then they should match and the decryption should be successful. However, if a computer is relocated to a second network, then the second network identifier will be different from the first network identifier and the authentication sequence will not be successfully decrypted. As such, an expedited login task will not be available and the user will have to do a complete new login in order to access network resources on the second network.

Kao merely describes the concept of storing encryption keys relative to passwords for a target resource. In particular, in paragraphs [0047] through [0051] recited by the Office Action above with respect to claims 1, 8, 15, and 20, *Kao* states as follows:

> [0047] However, in contrast to FIGS. 2B-2C, when a user's target password is stored or retrieved, it is encrypted or decrypted with the user's minor key, as described above with respect to FIG. 3A. In addition, rather than directly and insecurely storing the user's minor key, a storage key is generated; when storing and retrieving the user's minor key, the user's minor key is encoded and decoded to generate a storage key for the user, and the storage key is stored within the SSO database, as shown in FIG. 3B. The terms "storage key" and "encoded minor key" are thus interchangeable. Since the encoding function is quick and simple yet secure, very little computational effort is introduced when storing and retrieving a minor key.
>
> [0048] With reference now to FIG. 4, a flowchart depicts the process of establishing a data storage system including encoded minor keys in accordance with a preferred embodiment of the present invention. The process begins when a new user is being added to the system; the master key is first retrieved from the database (step 402). It may be assumed that the SSO server has already been installed and configured to generate and store a master key.
>
> [0049] A minor key is generated for the new user (step 404), and assuming that the user is also being provided with access to at least one restricted target resource, the user's target password is accepted or generated (step 406) and then encrypted with the user's minor key (step 408). The encrypted target password is then stored within the database (step 410) for use at a later time when the user actually attempts to access the restricted target resource.
>
> [0050] In order to keep the user's minor key confidentially and securely stored, the user's minor key is encoded with the master key (step 412) in order to generate an encoded minor key, i.e. the user's storage key. The storage key is then stored within the database (step 414), and the process of configuring an encrypted target password with an associated minor key is complete.
>
> [0051] With reference now to FIG. 5, a flowchart depicts the process of retrieving a target password stored within the SSO database in accordance with a preferred embodiment of the present invention. The process begins by retrieving the master key (step 502) and retrieving the user's encoded minor key, i.e. the user's storage key (step 504). The master key is used to decode the encoded minor key in order to regenerate the minor key (step 506). The decoded minor key is used to decrypt the user's encrypted target password (step 508). The target password is then provided to the target

> resource to authorize the user for access to the target resource (step 510), and the process is complete.

As set forth above, the user's target password used to access a restricted target resource on the network is encrypted using a "minor key." The user's minor key is then encoded with a master key so as to keep the user's minor key confidential and securely stored. In order to generate the encoded minor key, a storage key is employed that is stored in a database. Thus, all of the different encryption keys described by *Kao* are generated by network administrators or generated based upon other encryption keys. None of the encryption keys involve the use of a network identifier that identifies a network. Such is also the case with respect to claims 5, 6, and 7 that further define the nature of the network identifiers. None of this detail is shown or suggested by *Kao*. In addition, the use of network identifiers for encryption and decryption of authentication information is not shown or suggested.

Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn. In addition, Applicants respectfully request that the rejection of claims 8, 15, and 20 be withdrawn to the extent that they include subject matter similar in scope with that of claim 1. In addition, Applicant respectfully requests that the rejection of claims 3-7, 10-14, 17-19, 22, and 23 be withdrawn as depending from claims 1, 8, 15, or 20.

Next, in item 8 of the Office Action, claims 2, 9, 16, and 21 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kao* in view of U.S. Patent 5,166,979 issued to Takayama et al. (hereafter "*Takayama*"). A prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Rijckaert, 9 F.3d 1531, 28 U.S.P.Q2d 1955, 1956 (Fed. Cir. 1993). Applicants note that claims 2, 9, 16, and 21 depend from claims 1, 8, 15, and 20, respectively. Accordingly, Applicants assert that the cited combination of *Kao* and *Takayama* fails to show or suggest each of the elements of claims 2, 9, 16, and 21 as depending from claims 1, 8, 15, and 20 for the reasons described above with respect to claims 1, 8, 15, and 20. Accordingly, Applicants respectfully request that the rejection of claims 2, 9, 16, and 21 be withdrawn.

CONCLUSION

It is requested that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding this Response, the Examiner is encouraged to telephone the undersigned counsel of Applicants.

Respectfully submitted,

/Michael J. D'Aurelio/

Michael J. D'Aurelio
Registration Number: 40,977

Thomas, Kayden, Horstemeyer & Risley, L.L.P.
100 Galleria Parkway, N.W.
Suite 1750
Atlanta, Georgia 30339-5948
Phone: (770) 933-9500
Fax: (770) 951-0933